ANALISI STATICA E DINAMICA DEL FILE IEXPLORE.EXE

Introduzione

Come membro senior del SOC, è importante dimostrare al giovane dipendente che il file IEXPLORE.EXE trovato nella cartella C:\Program Files\Internet Explorer non è maligno, utilizzando strumenti di analisi statica e dinamica di base.

Analisi statica

1. **Verifica dell'hash del file:**
   - Generare l'hash SHA-256 del file IEXPLORE.EXE e confrontalo con un database di hash conosciuti di file legittimi. Questo può essere fatto utilizzando strumenti come `certutil` o `Get-FileHash` su Windows.

```
shell
certutil -hashfile "C:\Program Files\Internet Explorer\IEXPLORE.EXE"
SHA256
```

   Se l'hash corrisponde a quello di un file legittimo di Internet Explorer, è un buon indicatore della sua autenticità.

2. **Firma digitale:**
   - Controllare la firma digitale del file per verificare che sia stato firmato da Microsoft. Si può utilizzare `sigcheck` della suite Sysinternals o `Properties` nel menu contestuale del file in Windows Explorer.

```
shell
sigcheck -i "C:\Program Files\Internet Explorer\IEXPLORE.EXE"
```

   Una firma digitale valida da Microsoft conferma che il file non è stato alterato da quando è stato rilasciato da Microsoft.

3. **Metadata del file:**
   - Controllare le proprietà del file, come la versione, l'autore e i dettagli del prodotto. Queste informazioni possono essere visualizzate facendo clic con il pulsante destro del mouse sul file, selezionando "Proprietà" e navigando alla scheda "Dettagli".

   Un file legittimo di Internet Explorer avrà Microsoft Corporation come autore e dettagli del prodotto coerenti con Internet Explorer.

Analisi dinamica

1. **Esecuzione in un ambiente controllato:**
   - Eseguire il file in una macchina virtuale isolata e monitorane il comportamento. Utilizzare strumenti come `Process Monitor` della suite Sysinternals per osservare le attività del file, incluse le modifiche al file system, le chiavi di registro e le connessioni di rete.

```
shell
procmon
```

   Osservare se il comportamento del file è coerente con quello di un browser legittimo. Un comportamento anomalo potrebbe indicare che il file è stato compromesso.

2. **Monitoraggio delle connessioni di rete:**
   - Utilizzare strumenti come `Wireshark` o `Netstat` per monitorare le connessioni di rete stabilite dal file IEXPLORE.EXE. Un browser legittimo stabilirà connessioni a siti web conosciuti e servizi di Microsoft.

```
shell
netstat -an | findstr "iexplore.exe"
```

   Connessioni a indirizzi IP o domini sospetti potrebbero indicare attività malevole.

3. **Utilizzo del task manager e monitor delle risorse:**
   - Osservare l'uso delle risorse del sistema da parte del file IEXPLORE.EXE utilizzando il Task Manager o il Monitor delle Risorse. Un uso elevato e ingiustificato delle risorse potrebbe indicare un comportamento sospetto.

```
shell
taskmgr
```

   Controllare che il processo sia coerente con quello di un browser in esecuzione.

Conclusione

Seguendo questi passaggi, si può dimostrare che il file IEXPLORE.EXE nella directory specificata è il legittimo eseguibile di Internet Explorer di Microsoft. Utilizzando strumenti di analisi statica per verificare l'hash e la firma digitale, e strumenti di analisi dinamica per monitorare il comportamento del file in esecuzione, possiamo garantire al dipendente che il file non è maligno.

Se tutti i controlli sopra menzionati confermano che il file è legittimo e non presenta comportamenti anomali, il dipendente può essere rassicurato della sua autenticità.